(12) UK Patent Application (19) GB (11) 2 348 036 (13) A

(43) Date of A Publication 20.09.2000

(21) Application No 9905924.8

(22) Date of Filing 15.03.1999

(71) Applicant(s)
Tony Evans
26 Bloomsbury Square, LONDON, WC1A 2VJ, United Kingdom

Kevin Hutchinson
9 Noel Road, Islington, LONDON, N1 8HQ, United Kingdom

(72) Inventor(s)
Tony Evans
Kevin Hutchinson

(74) Agent and/or Address for Service
Hillgate Patent Services
No 6 Aztec Row, Berners Road, Islington, LONDON, N1 0PW, United Kingdom

(51) INT CL[7]
G07F 7/08

(52) UK CL (Edition R)
G4V VAK

(56) Documents Cited
GB 2252270 A WO 98/43825 A1 WO 97/26618 A1
US 5432506 A US 3833795 A

(58) Field of Search
UK CL (Edition Q) G4V VAK
INT CL[6] G07F 7/02 7/08

(54) Abstract Title
Coded voucher for preventing transaction fraud

(57) A method for allowing a transaction comprises providing, e.g. to a sales point, a voucher bearing a voucher code, deriving an authentication code from the voucher code at a separate later stage, e.g. when it is sold to a user, and marking the voucher with the authentication code so that when the voucher is used during the transaction its validity may be ascertained by checking that the authentication code has been derived from the voucher code. Preferably the voucher represents money and the transaction includes the payment of some or all of the voucher's worth. The voucher may be marked by a plurality of authentication codes, one of which is initially hidden, e.g. by a scratch off layer or a tear off strip, and may only be revealed in an irreversible manner. The voucher's monetary worth may be derivable from the voucher code and the codes may be printed as numbers, bar codes, or stored in a chip. The transaction may be performed over a communication link, e.g. the internet, and may be a purchase, a loyalty scheme, or a corporate voucher scheme. The voucher may be a smart card, a piece of printed cardboard or paper, or may not have a physical form.

GB 2 348 036 A

Payment Instruments

The Internet allows an unprecedented degree of access to information and interaction with other people, the geographical location generally being irrelevant. It has also been hailed as starting a similar commercial revolution, but as yet this has not materialised. Not only has the total amount of trade been disappointing, but much of this has relied upon the reputation of the traders outside the world of the Internet.

When a potential purchaser wishes to buy a product or service which he sees offered over the Internet, the usual method is to give details of his credit card. Understandably, people are reluctant to do this, as once a supplier has credit card details there is an opportunity for fraud, and it may be difficult to ascertain the suppliers geographical location. Additionally, credit card details may be intercepted by third parties intent on fraud. Debit cards are similarly vulnerable.

In any case, in order to effect a transaction using a credit card the purchaser must own a credit card, and the vendor must have merchant status to accept credit card transactions. A significant number of people are refused, or choose not to own a credit card, and it may be difficult for a small business persuade banks to grant them merchant status for Internet business.

To keep credit transactions on the web secure, complex encryption systems are required. Nevertheless, people remain wary of buying products over the web from unseen vendors using credit cards.

The object of the present invention is to provide a system for allowing transactions to be conducted over the web in a secure and efficient manner.

According to the present invention there is provided a method for allowing a transaction, including

providing a voucher bearing a voucher code,

marking said voucher by a code derivation means at a separate, later stage with a authentication code which is derivable from the voucher code,

the voucher code and the authentication code being supplied to a verification means capable of checking that the authentication code has been derived from the voucher code, the verification means, on confirming this, indicating that the code is authentic.

Preferably the voucher represents a monetary denomination. Preferably the transaction includes the authorisation of an amount equal to all or part of the voucher's denomination to be used as payment.

Preferably the voucher is marked by two separate authentication codes which are derivable from the voucher code, one of which is initially hidden, and may only be revealed in an irreversible manner. Preferably the voucher's monetary denomination is derivable from the voucher code. Preferably the payment is executed over a communication link, particularly the Internet.

According to another aspect of the present invention, there is provided a voucher as defined above.

According to another aspect of the present invention, there is provided a key derivation means as defined above.

According to another aspect of the present invention, there is provided a verification means as defined above.

A payment method will now be described, by way of example.

The voucher is a rectangular piece of cardboard, the size of a credit card, upon which is printed three labelled boxes, a Title, and a denomination. The three boxes comprise an Hidden code box, Serial code box, and Key code box, and are labelled as such. The Hidden code box and Serial code box are printed with two strings of characters, whilst at this stage the Key code is left blank. The Hidden code box is then masked by covering it with a removable surface of the scratchcard type, that is, when the surface is scratched, the printed matter beneath is revealed.

The Hidden code is a four character alphanumeric code, excluding both the letters 'O' and 'I' and the numbers nought and one in order to avoid confusion. The Serial code is an eight figure code uniquely identifying each card printed. The Serial codes are not a consecutive series of integers, but occur at intervals from a series of consecutive integers. This is known as a sparse series. The intervals are either random or generated by an algorithm, but in either the case the particular series is known to scheme's organisers.

The voucher may be purchased over the counter from a shop. The cards are provided to the shop with the Key code box left empty, but the shop is equipped with a machine such as a programmed cash register or computer which will supply a Key code. Each machine uses an algorithm to generate a Key code from the Serial code, these machines hereafter being called Key Cutting machines. When a card is being purchased, the Key Cutting machine is used to obtain the Key code for the card, and written, or preferably printed, in the Key code box. The Key code, like the Hidden code, is a four character alphanumeric code.

The Serial code is simply a unique identifier allocated to each card. Its relationship with the Key code must however be made very difficult to ascertain. The voucher may now be used to make purchases at other shops over the counter, and the Key code may be used, if necessary, to demonstrate that the card was properly issued, by entering the Serial code in the shop's Key cutting machine. In order to use the card for such a

purchase, the Hidden code box must not have been revealed, as removal of the masking indicates that the card may have been used for an Internet purchase, the process of which is explained below. When the purchase is made, the voucher is surrendered, with change or lower denomination vouchers being given to make up any difference between the difference in the voucher's value and the value of the purchase. The vendor may now arrange for the voucher to be exchanged with the organisers of the voucher system.

In order to make a purchase over the Internet, the voucher holder must reveal the Hidden code printed in the Hidden code box. When the voucher holder visiting the vendor's server decides to make a purchase he is connected to the authentication scheme site run by the organisers of the voucher system, hereinafter called the Voucher Server.

The voucher holder then enters the Hidden code, the Serial code and the Key code which is sent to the Voucher Server, using a conventional encryption scheme for extra security. The Voucher Server checks that the stated Serial code is an element of the sparse series set, and that Hidden code and Key code correctly correspond to this Serial code. An account corresponding to the Serial code is set up for the voucher's monetary denomination, if no such account has already been set up. Money from this account may then be used to pay for the Internet purchase. If the full amount of the account is not spent on the first purchase, then the Voucher server may be visited on subsequent occasions, again checking that the Hidden code and Key code correspond to the Serial code, so that the voucher holder may make subsequent purchases until the account is exhausted.

Some or all the money in one account could be transferred to another account upon production of the first accounts Serial code, Key code and Hidden code, so that small amounts remaining from previous purchases can be collected up from different accounts, or a large total can be amassed for an expensive purchase.

The Hidden code is derivable from the Serial code by an algorithm in a similar way to the relationship between the Serial code and the Key code. The Voucher Server checks that both the Key code and the Hidden code correspond to the Serial code.

Alternatively, either the Hidden code or the Key code could be derived from a table of all the Serial codes and corresponding codes, there being no algorithmic relationship between the Serial code and the corresponding code or codes. Each Key cutting machine must then be supplied with such a table, or else be equipped with a link to the Voucher server.

It will be apparent to one buying a valid voucher that it could not have been used for an Internet transaction, for the Hidden code box's mask should be intact. Also, that the clear Key box (and the fact that the vendor must exchange the voucher for payment by the organisers of the voucher system) indicate that the voucher has not been used in a over the counter purchase. It is also reassuring with a customer that even if a fraud were to be perpetrated, he could never be liable for more than the value of the voucher.

The vendor will be similarly reassured by the intact mask of the Hidden code box that it has not been previously used in an Internet purchase. Since unissued vouchers, having no Key code written upon them, cannot be used for payment, they should not attract the attentions of thieves. The security of the Key cutting machines, and their algorithms (or tables if used), is paramount. Precautions must be taken to protect the key cutting machines and the algorithms, such as monitoring the whereabouts of the Key cutting machines, and making sure that the Hidden codes are concealed as soon as possible after being printed. The algorithms or tables used by the Voucher server should also be secured, for example by keeping separate the programming from the code tables.

The Serial codes are themselves generated by an algorithm or from a table in order to achieve the sparse spacing. The Key cutting machine will

also check that the Serial code submitted exists. Affirmation of this, and the giving of the Key code, will be artificially delayed, say by five seconds. In this way, if a Key cutting machine is compromised, obtaining a list of usable Serial codes and the corresponding Key codes will be made more difficult.

The Key cutting machines, if linked to the Voucher Server or another centralised site, may also be used to audit the system, by logging the Serial code of each voucher used for over the counter purchases. This may be combined with Serial code data from vouchers used to set up accounts at the Voucher server. As an additional check a verification request may be sent from the Key cutting machine to the Voucher Server, and the Serial code checked against such data to check that the Serial code has not already been used to initiate an account.

The Serial code and a single derived code could be printed on the voucher, and the voucher confined to either a system solely for Internet transactions, or a system solely for over-the-counter transactions. The derived code could be initially masked in some way.

The vouchers could be used in a corporate voucher system within a single company, or between companies, wherein members of a company receive the vouchers as, say, an incentive or bonus, and may be used within or between companies. The voucher does not then have to be for a specific denomination, but could signify simply that the holder is entitled to some preferential treatment, the Key code showing that the voucher has been correctly issued. Such non-denomination vouchers could indeed be used in a similar way for a public voucher system.

A company having both shops and an Internet presence could issue its own vouchers to be used either in its shops or to buy products from its Internet server. The Voucher Server could then be organised by the company itself and incorporated into the company's Internet server.

Numerous variations relying upon the principles herein disclosed are possible. The physical form of the voucher could be varied considerably, for instance it could be a piece of printed paper similar in size to a banknote, or indeed need not be in a physical form at all.

The Serial code, Hidden code, and Key code could be printed as a machine-readable bar code, or supplied upon a chip incorporated in the card, in addition to or instead of being provided in a form immediately apparent to a person. The method of masking the Hidden code could be a tear of strip or other suitable means. The precise length and type of characters used in the codes could easily be adapted according to the circumstances. Other encryption techniques could if desired be incorporated into the voucher.

The voucher system could easily be adapted to allow transactions over any type of net, or even for telephone transactions.

CLAIMS

1. A method for allowing a transaction, including

providing a voucher bearing a voucher code,

marking said voucher by a code derivation means at a separate, later stage with a authentication code which is derivable from the voucher code,

the voucher code and the authentication code being supplied to a verification means capable of checking that the authentication code has been derived from the voucher code, the verification means, on confirming this, indicating that the code is authentic.

2. A method according to the previous claim, wherein the voucher represents a monetary denomination.

3. A method according to claim 2, wherein the transaction includes the authorisation of an amount equal to all or part of the voucher's denomination to be used as payment.

4. A method according to any previous claim, wherein the voucher is marked by two or more separate authentication codes which are derivable from the voucher code, one of which is initially hidden, and may only be revealed in an irreversible manner.

5. A method according to any previous claim, wherein the voucher's monetary denomination is derivable from the voucher code.

6. A method according to any any of claims 3 to 5, wherein the payment is executed over a communication link, particularly the Internet.

7. A voucher according to any previous claim.

8. A key derivation means according to any of claims 1 to 6.

9. A verification means according to any of claims 1 to 6.

10. A method for allowing a transaction substantially as herein described and illustrated.

11. A voucher substantially as herein described and illustrated.

12. A key derivation means substantially as herein described and illustrated.

13. A verification means substantially as herein described and illustrated.

14. Any novel and inventive feature or combination of features specifically disclosed herein within the meaning of Article 4H of the International Convention (Paris Convention).

The Patent Office

INVESTOR IN PEOPLE

Application No: GB 9905924.8 **Examiner:** Dr. Andrew Glanfield
Claims searched: 1-7, 10-11 **Date of search:** 28 June 1999

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): G4V (VAK)

Int Cl (Ed.6): G07F (7/02, 7/08)

Other: ONLINE: EPODOC, JAPIO, WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
A	GB 2252270 A	(WREN-HILTON) see whole document.	4, 7
A	WO 9843825 A1	(AARON) see whole document.	4-6, 7
X	WO 9726618 A1	(MERRILL LYNCH) see whole document.	1-3, 7
X	US 5432506	(CHAPMAN) see whole document.	1-3, 7
A	US 3833795	(ELSCINT) see whole document.	1, 7

X Document indicating lack of novelty or inventive step
Y Document indicating lack of inventive step if combined with one or more other documents of same category.
& Member of the same patent family
A Document indicating technological background and/or state of the art.
P Document published on or after the declared priority date but before the filing date of this invention.
E Patent document published on or after, but with priority date earlier than, the filing date of this application.